

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-108395

(43)Date of publication of application : 10.04.2002

(51)Int.Cl. G10L 19/00
G11B 20/10
H03M 7/30

(21)Application number : 2000-296871 (71)Applicant : KOBE STEEL LTD

(22)Date of filing : 28.09.2000 (72)Inventor : MORITA KOJI
HASHIMOTO HIROSHI
SHIMODA TOSHIAKI

(54) DIGITAL MUSIC REPRODUCING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a digital music reproducing device which can prevent data having been decoded from being read out of a circuit.

SOLUTION: This device is equipped with a circuit for decoding a code and a circuit for expanding compression in the same computing element and supplies data having been decoded to the circuit which expands the compression through an internal path of the computing element to prevent the data having been decoded from being read out of the circuit.

CLAIMS

[Claim(s)]

[Claim 1] A code decoding circuit which performs code decryption about digital music data by which compression encryption was carried out. Have a compression restoration circuit which elongates data by which code decryption was carried out in said code decoding circuit and restores the original digital music data and by said compression restoration circuit. In a digital music reproduction device which plays restored digital music data. A digital music reproduction device which supplies data by which was provided with said code decoding circuit and said compression restoration circuit in the same arithmetic element and code decryption was carried out in said code decoding circuit to said compression restoration circuit through an internal bus of

said arithmetic element and is characterized by things.

[Claim 2] Although said code decoding circuit performs code decryption about said digital music data by which compression encryption was carried out. The digital music reproduction device according to claim 1 which is provided also with a code decoding data recording memory which records code decoding data to be used in said arithmetic element and supplies said code decoding data to said code decoding circuit from said code decoding data recording memory through an internal bus of said arithmetic element.

[Claim 3] A digital-to-analog converter which changes into an analog signal said digital music data restored by said compression restoration circuit is also provided with it in said arithmetic element and by said compression restoration circuit. The digital music reproduction device according to claim 1 or 2 which supplies said restored digital music data to said digital-to-analog converter through an internal bus of said arithmetic element.

[Claim 4] A compression restoration program which said compression restoration circuit uses. It has a recording memory in said arithmetic element temporarily [volatile / compression restoration program] which records a part of compression restoration programs recorded on a nonvolatile compression restoration program documentation memory to record. The digital music reproduction device according to claim 1 which supplies said a part of compression restoration programs to said compression restoration circuit from a recording memory temporarily [said / compression restoration program].

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] The code decoding circuit which performs code decryption about the digital music data in which compression encryption of this invention was carried out. It has a compression restoration circuit which elongates the data by which code decryption was carried out in said code decoding circuit and restores the original digital music data and is related with the digital music reproduction device which plays the digital music data restored by said compression restoration circuit.

[0002]

[Description of the Prior Art] For example, there are various compression encoding systems in digital music data such as MP3 and TwinVQ. These compression encoding systems made possible music reproduction of quality comparatively sufficient also by a narrow band or small capacity and brought about the rapid spread of the digital music reproduction devices which play digital music data. Said digital music reproduction device performs decryption corresponding to the compression encoding

system used for carrying out compression encoding of the digital music data elongates data and is provided with the compression restoration circuit which restores the original digital data. In said digital music reproduction device corresponding to various compression encoding systems an arithmetic element programmable as said compression restoration circuit is used in many cases. Record on the memory two or more compression restoration programs which described the procedure for restoring the original digital music data corresponding to two or more compression encoding systems and one of compression restoration programs is loaded at the time of necessity. Processing which restores the original digital music data by said arithmetic element is performed. In said digital music reproduction device the copyright about digital music data poses a problem. Since the digital music data by which compression encoding was carried out has small capacity time required for a duplicate is short and since the compression encoding system usually used is restricted it is simple also for reproduction of what was reproduced. Of course since it is digital data there is also no tone quality degradation which is produced when reproducing an analog signal. Therefore a possibility that the almost same thing as original music may be distributed by the illegal duplicate is also high. For this reason there is also a digital music reproduction device which enabled it to play about the digital (compression encoding and encryption were performed) music data by which compression encryption was carried out beforehand. After decrypting a code to the digital music data by which compression encryption was carried out beforehand according to the specification of a code the data (data which compressed digital music data of a yuan) obtained by it is elongated and the original digital music data is restored. If compression encryption is carried out beforehand even if the data is reproduced the original digital music data cannot be obtained.

[0003]

[Problem(s) to be Solved by the Invention] If the digital music data which is not enciphered from the first and digital music data after code decryption was performed can be dealt with freely it can perform reproducing illegally or distributing now easily and development of music culture and by extension development of the digital music industry will also be barred. However in the digital music reproduction device which enabled it to play the digital music data by which compression encryption was carried out beforehand it was carried out to extension of compressed data using the arithmetic element in which the thing using a programmable arithmetic element of extension of compressed data and decryption of a code is also separate. That is data after code decryption was performed on the data bus which appears in the electric circuit is flowing as it is. It is not impossible to read the data which flows on the data bus which connects between separate arithmetic elements and there is a possibility that data after code decryption was performed and by extension the original digital music data may be reproduced unjustly. This invention is made in view of the technical problem in such a Prior art and an object of this invention is to provide the

digital music reproduction device which can prevent data after code decryption was performed from being read in on a circuit.

[0004]

[Means for Solving the Problem] A code decoding circuit which performs code decryption about digital music data in which compression encryption of this invention was carried out in order to attain the above-mentioned purpose. Have a compression restoration circuit which elongates data by which code decryption was carried out in said code decoding circuit and restores the original digital music data and by said compression restoration circuit. In a digital music reproduction device which plays digital music data which plays restored digital music data. It has said code decoding circuit and said compression restoration circuit in the same arithmetic element and is constituted as a digital music reproduction device which supplies data by which code decryption was carried out in said code decoding circuit to said compression restoration circuit through an internal bus of said arithmetic element and is characterized by things. A code decoding circuit which performs code decryption in a digital music reproduction device concerning this invention about digital music data by which compression encryption was carried out. Data in which it had a compression restoration circuit which elongates data by which code decryption was carried out in said code decoding circuit and restores the original digital music data in the same arithmetic element and code decryption was carried out by said code decoding circuit is supplied to said compression restoration circuit through an internal bus of said arithmetic element. For this reason, data by which code decryption was carried out in said code decoding circuit can prevent data after being unable to acquire directly from a bus of the exterior of said arithmetic element but performing code decryption from being read in on a circuit. However, if code decoding data used for performing said code decryption can acquire from a bus of the exterior of said arithmetic element even if data by which code decryption was carried out even if cannot acquire from a bus of the exterior of said arithmetic element. From digital music data by which compression encryption was carried out, a possibility that the original digital music data may be restored using said code decoding data remains. Then, although said code decoding circuit performs code decryption in said digital music reproduction device about said digital music data by which compression encryption was carried out. It also has a code decoding data recording memory which records code decoding data to be used in said arithmetic element and may be made to supply said code decoding data to said code decoding circuit from said code decoding data recording memory through an internal bus of said arithmetic element. In this case, code decoding data used for performing code decryption cannot be acquired from a bus of the exterior of said arithmetic element, either, but can prevent a duplicate of the original digital music data more strongly.

[0005] If that to which capacity becomes large and said digital music data restored by said compression restoration circuit requires time for a duplicate will be

reproduced there will be no change in the same thing as an almost original thing being obtained. Then in said digital music reproduction device by for example said compression restoration circuit. A digital-to-analog converter which changes said restored digital music data into an analog signal is also provided with it in said arithmetic element and by said compression restoration circuit. It may be made to supply said restored digital music data to said digital-to-analog converter through an internal bus of said arithmetic element. In this case from a bus of the exterior of said arithmetic element said digital music data restored by said compression restoration circuit cannot be acquired either but can make that unjust reproduction more difficult. In said digital music reproduction device in order to correspond to two or more compression encoding systems two or more compression restoration programs which said compression restoration circuit uses may be prepared but. Since a comparatively high-speed volatile memory is expensive when it is going to hold down cost a nonvolatile comparatively low speed memory will be used. However if said compression restoration program is supplied to said compression restoration circuit from a nonvolatile comparatively low speed memory processing speed will fall. Then a part of compression restoration programs recorded on a nonvolatile compression restoration program documentation memory which records a compression restoration program which said compression restoration circuit uses in said digital music reproduction device temporarily [volatile / compression restoration program] to record a recording memory. It has in said arithmetic element and may be made to supply said a part of compression restoration programs to said compression restoration circuit from a recording memory temporarily [said / compression restoration program]. In this case temporarily [said / compression restoration program] to a recording memory. What is necessary is to secure only capacity which records a part of compression restoration programs memorized by said compression restoration program documentation memory and said a part of compression restoration programs. Since it is supplied from a recording memory temporarily [comparatively high-speed / volatile / compression restoration program] high-speed processing is realizable holding down cost.

[0006]

[Embodiment of the Invention] Hereafter with reference to an accompanying drawing it explains per embodiment of the invention and an understanding of this invention is presented. Following embodiments are the concrete examples of this invention and are not the things of the character which limits the technical scope of this invention. It is a figure showing the outline composition of the digital music reproduction device which drawing 1 requires at an embodiment of the invention here. As shown in drawing 1 the digital music reproduction device concerning an embodiment of the invention consists of the digital music data recording memory 101 the arithmetic element 102 the compression restoration program documentation memory 103 D/A converter 104 the analog circuitry 105 etc. The digital music data recording memory 101 is a memory for

storing the digital music data by which compression encryption was carried out and is connected to the arithmetic element 102. The arithmetic element 102 performs processing which restores the digital music data from the digital music data recording memory 101 to the original digital music data before compression encryption is carried out and is connected to D/A converter 104. It is connected to the exterior of the arithmetic element 102 and the compression restoration program documentation memory 103 supplies the compression restoration program which performs decryption corresponding to the compression encoding system which carried out compression encoding of said digital music data to the arithmetic element 102. D/A converter 104 changes into an analog signal the digital music data supplied from the arithmetic element 102 and is connected to the analog circuitry 105. After the analog circuitry 105 connects D/A converter 104 and a loudspeaker and processes amplification etc. if needed it inputs the analog signal from D/A conversion 104 into a loudspeaker.

[0007] The arithmetic element 102 of each composition mentioned above serves as the principal part of the digital music reproduction device concerning an embodiment of the invention. The internal configuration of the arithmetic element 102 is also shown in drawing 1. As shown in drawing 1 the arithmetic element 102 contains the data input circuit 11, the code decoding circuit 12, the compression restoration circuit 13, a data output circuit and the code decoding data recording memory 21 in the inside. The data input circuit 11 is an interface for inputting into the arithmetic element 102 the digital music data by which was connected with the digital music data recording memory 101 and compression encryption was carried out from the digital music data recording memory 101. The code decoding circuit 12 is a circuit which decrypts the code of the digital music data which was inputted from the data input circuit 11 and by which compression encryption was carried out using the code decoding data recorded on the code decoding data recording memory 21. The compression restoration circuit 13 is a circuit which elongates the data by which code decryption was carried out in the code decoding circuit 12 using the compression restoration program recorded on the compression restoration program documentation memory 103 and restores the original digital music data before compression. The data output circuit 11 is an interface for outputting the digital music data obtained by the compression restoration circuit 13 to D/A converter 104. The code decoding data recording memory 21 is a memory which records the code decoding data for code decryption and supplies said code decoding data to the code decoding circuit 12. For example when using the common key encryption system—ized method by DES the common key which should be made secret is recorded on the code decoding data recording memory 21 the parameter data [for a DES code] and cipher—processing side. Each composition in the above arithmetic elements 102 with an internal bus (it expresses with the arrow which is in said arithmetic element 102 for convenience at drawing 1). It is connected and only the data inputted into the data input circuit 11, the data outputted from the data output circuit 14 and a compression

restoration program are obtained from the connection passage of the arithmetic element 102 exterior. Since [for it / in which it is simple to restore the original digital music data] it is restricted and the capacity of data of the compression encoding system which that into which the data outputted is compressed is not enciphered but is well used from the code decoding circuit 12 is also comparatively small it is easy to reproduce. Such data also passes only through the internal bus of the arithmetic element 102 and is concealed from the outside. The code decoding data currently recorded on the code decoding data recording memory 21 also passes only through an internal bus and is concealed from the outside. If the code decoding data of the code decoding data recording memory 21 is acquired unjustly even if only the digital music data by which compression encryption was carried out will be obtained the original digital music data will be restored simply but. Such a situation is also prevented by concealing code decoding data from the outside. Thus in the digital music reproduction device concerning an embodiment of the invention. Since the data by which the code decoding circuit and the compression restoration circuit are provided in the same arithmetic element and code decryption was carried out in said code decoding circuit is supplied to said compression restoration circuit through the internal bus of said arithmetic element The data in which code decryption was performed can be prevented from being read in on a circuit. Since it also has said code decoding data storage memory in said arithmetic element and said code decoding data is supplied to said code decoding circuit from said code decoding data storage memory through the internal bus of said arithmetic element Said code decoding data which is needed for restoring the original digital music data from the data by which compression encryption was carried out can also be concealed from the outside.

[0008]

[Example] Although said compression restoration program was directly supplied to the compression restoration circuit 13 in said embodiment from the compression restoration program documentation memory 103 arranged to the exterior of the arithmetic element 102 For example as shown in drawing 2 said compression restoration program. The recording memory 31 is formed in the arithmetic element 102 temporarily [volatile / compression restoration program] are recorded temporarily Make the recording memory 31 memorize said required compression restoration program of said compression restoration programs memorized by the compression restoration program documentation memory 103 temporarily [compression restoration program] and the compression restoration program concerned temporarily [compression restoration program] the recording memory 31. [two or more] It leads and may be made to supply the compression restoration circuit 13. In order to perform more nearly high-speed processing it is preferred to read said compression restoration program from a high-speed memory but it will become difficult to hold down cost if it is going to secure capacity required [the high-

speed volatile memory is expensive and] in order to memorize said many of compression restoration programs. On the other hand since the nonvolatile low speed memory is comparatively cheap cost can be held down even if it increases the capacity of the compression restoration program documentation memory 103. ThereEither which is memorized by the compression restoration program documentation memory 103Or the capacity which memorizes only said a part of compression restoration programs is secured to the recording memory 31 temporarily [compression restoration program]and said compression restoration program which the compression restoration circuit 13 uses is supplied from the recording memory 31 temporarily [compression restoration program]. If the capacity of the compression restoration program documentation memory 103 is a grade which can store a small number of compression restoration programhigh-speed processing can be realized so greatly [increase of cost]holding down cost. Although D/A converter 104 is arranged to the exterior of the arithmetic element 102 in said embodimentFor exampleD/A converter 104 is also formed in arithmetic element 102 insideand it may be made to supply the digital music data outputted from the data output circuit 14 to D/A converter 41 through the internal bus of the arithmetic element 102as shown in drawing 3. If that to which capacity becomes large and said digital music data outputted from the data output circuit 14 requires time for a duplicate will be reproducedthere will be no change in the same thing as an almost original thing being obtained. Therefore said digital music data is also concealed by supplying the digital music data outputted to D/A converter 41 through the internal bus of the arithmetic element 102 from the data output circuit 14. By thisunjust reproduction can be made more difficult.

[0009]

[Effect of the Invention]According to the digital music reproduction device concerning this inventionas explained above. The code decoding circuit which performs code decryption about the digital music data by which compression encryption was carried outThe compression restoration circuit which elongates the data by which code decryption was carried out in said code decoding circuitand restores the original digital music data is provided with it in the same arithmetic elementand by said code decoding circuit. Since the data by which code decryption was carried out is supplied to said compression restoration circuit through the internal bus of said arithmetic elementit can prevent data after code decryption was carried out from being read in on a circuit. Although said code decoding circuit performs code decryption in said digital music reproduction device about said digital music data by which compression encryption was carried out. If it also has a code decoding data recording memory which records the code decoding data to be used in said arithmetic element and it supplies said code decoding data to said code decoding circuit from said code decoding data recording memory through the internal bus of said arithmetic elementThe code decoding data used for performing code decryption cannot be

acquired from the bus of the exterior of said arithmetic element either but can prevent the duplicate of the original digital music data more strongly. In said digital music reproduction device by for example said compression restoration circuit. The digital-to-analog converter which changes said restored digital music data into an analog signal is also provided with it in said arithmetic element and by said compression restoration circuit. If said restored digital music data is supplied to said digital-to-analog converter through the internal bus of said arithmetic element From the bus of the exterior of said arithmetic element said digital music data restored by said compression restoration circuit cannot be acquired either but can make the unjust reproduction more difficult. A part of compression restoration programs recorded on the nonvolatile compression restoration program documentation memory which records the compression restoration program which said compression restoration circuit uses in said digital music reproduction device temporarily [volatile / compression restoration program] to record a recording memory. It has in said arithmetic element and said a part of compression restoration programs can realize high-speed processing holding down cost if said compression restoration circuit is supplied from a recording memory temporarily [said / compression restoration program].

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The figure showing the outline composition of the digital music reproduction device concerning an embodiment of the invention.

[Drawing 2] The figure showing the outline composition of the digital music reproduction device concerning one example of this invention.

[Drawing 3] The figure showing the outline composition of the digital music reproduction device concerning other examples of this invention.

[Description of Notations]

12 -- Code decoding circuit

13 -- Compression restoration circuit

21 -- Code decoding data recording memory

31 -- Compression restoration program one time recording memory

102 -- Arithmetic element

104 -- D/A converter

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2002-108395
(P2002-108395A)

(43)公開日 平成14年 4月10日 (2002. 4. 10)

(51)Int.Cl. ⁷	識別記号	F I	テームコード*(参考)
G 1 0 L 19/00		G 1 1 B 20/10	H 5 D 0 4 4
G 1 1 B 20/10		H 0 3 M 7/30	Z 5 D 0 4 5
H 0 3 M 7/30		G 1 0 L 9/18	M 5 J 0 6 4
		9/00	N
		9/18	H
審査請求 有 請求項の数3 O L (全 8 頁)			

(21)出願番号 特願2000-296871(P2000-296871)

(22)出願日 平成12年 9月28日 (2000. 9. 28)

(71)出願人 000001199
株式会社神戸製鋼所
兵庫県神戸市中央区脇浜町 1丁目 3番18号
(72)発明者 森田 孝司
兵庫県神戸市西区高塚台 1丁目 5番 5号
株式会社神戸製鋼所神戸総合技術研究所内
(72)発明者 橋本 裕志
兵庫県神戸市西区高塚台 1丁目 5番 5号
株式会社神戸製鋼所神戸総合技術研究所内
(74)代理人 100084135
弁理士 本庄 武男

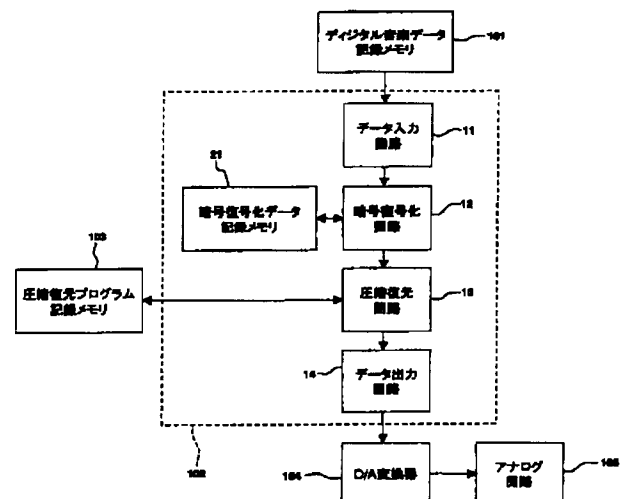
最終頁に続く

(54)【発明の名称】 デジタル音楽再生装置

(57)【要約】

【課題】 暗号の復号化と圧縮の伸長を行ってデジタル音楽データを再生する従来のデジタル音楽再生装置では、暗号を復号化する処理と圧縮の伸長を行う処理とが別個の素子により行われており、電気回路のデータバス上で暗号の復号化が行われた後のデータが読み取られる恐れがあった。

【解決手段】 本発明は、暗号の復号化を行う回路と圧縮の伸長を行う回路とを同一の演算素子内に備え、暗号の復号化が行われた後のデータを前記演算素子の内部バスを通じて圧縮の伸長を行う回路に供給することにより、暗号の復号化が行われた後のデータが回路から読み取られることを防止することを図ったものである。



【特許請求の範囲】

【請求項1】 圧縮暗号化されたデジタル音楽データについて暗号復号化を行う暗号復号化回路と、前記暗号復号化回路により暗号復号化されたデータを伸長して元のデジタル音楽データを復元する圧縮復元回路とを備え、前記圧縮復元回路により復元されたデジタル音楽データを再生するデジタル音楽再生装置において、前記暗号復号化回路と前記圧縮復元回路とを同一の演算素子内に備え、前記暗号復号化回路により暗号復号化されたデータを前記演算素子の内部バスを通じて前記圧縮復元回路に供給してなることを特徴とするデジタル音楽再生装置。

【請求項2】 前記暗号復号化回路が前記圧縮暗号化されたデジタル音楽データについて暗号復号化を行うのに用いる暗号復号化データを記録する暗号復号化データ記録メモリも前記演算素子内に備え、前記演算素子の内部バスを通じて前記暗号復号化データを前記暗号復号化データ記録メモリから前記暗号復号化回路に供給してなる請求項1記載のデジタル音楽再生装置。

【請求項3】 前記圧縮復元回路により復元された前記デジタル音楽データをアナログ信号に変換するデジタルアナログ変換器も前記演算素子内に備え、前記圧縮復元回路により復元された前記デジタル音楽データを前記演算素子の内部バスを通じて前記デジタルアナログ変換器に供給してなる請求項1又は2記載のデジタル音楽再生装置。

【請求項4】 前記圧縮復元回路が利用する圧縮復元プログラムを記録する不揮発性の圧縮復元プログラム記録メモリに記録された一部の圧縮復元プログラムを記録する揮発性の圧縮復元プログラム一時記録メモリを前記演算素子内に備え、前記一部の圧縮復元プログラムは前記圧縮復元プログラム一時記録メモリから前記圧縮復元回路に供給してなる請求項1記載のデジタル音楽再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、圧縮暗号化されたデジタル音楽データについて暗号復号化を行う暗号復号化回路と、前記暗号復号化回路により暗号復号化されたデータを伸長して元のデジタル音楽データを復元する圧縮復元回路とを備え、前記圧縮復元回路により復元されたデジタル音楽データを再生するデジタル音楽再生装置に関するものである。

【0002】

【従来の技術】 例えばMP3 やTwinVQなど、デジタル音楽データには様々な圧縮符号化方式がある。これらの圧縮符号化方式は、比較的狭い帯域や小さな容量でも十分な品質の音楽再生を可能とし、デジタル音楽データを再生するデジタル音楽再生装置の急速な普及をもたらした。前記デジタル音楽再生装置は、デジタル音楽

データを圧縮符号化するのに用いられた圧縮符号化方式に対応する復号化を行ってデータを伸長し、元のデジタルデータを復元する圧縮復元回路を備える。多様な圧縮符号化方式に対応する前記デジタル音楽再生装置では、前記圧縮復元回路としてプログラマブルな演算素子が用いられることも多い。複数の圧縮符号化方式に対応して元のデジタル音楽データを復元するための手順を記述した複数の圧縮復元プログラムをメモリに記録しておき、必要時にいずれかの圧縮復元プログラムをロードして、前記演算素子により元のデジタル音楽データを復元する処理を行うのである。前記デジタル音楽再生装置において問題となるのが、デジタル音楽データについての著作権である。圧縮符号化されたデジタル音楽データは容量が小さいため、複製に必要な時間は短く、通常利用される圧縮符号化方式は限られているから、複製したものの再生も簡単である。もちろん、デジタルデータであるから、アナログ信号を複製する際に生じるような音質劣化もない。従って、違法な複製によって、オリジナルの音楽とほとんど同じものが頒布される恐れも高い。このため、予め圧縮暗号化された（圧縮符号化と暗号化が行われた）デジタル音楽データについて再生を行い得るようにしたデジタル音楽再生装置もある。予め圧縮暗号化されたデジタル音楽データに対して、暗号の仕様に従って暗号の復号化を行ってから、それによって得たデータ（元のデジタル音楽データを圧縮したデータ）を伸長して、元のデジタル音楽データを復元するのである。予め圧縮暗号化されていれば、そのデータが複製されても、元のデジタル音楽データを得ることができない。

【0003】

【発明が解決しようとする課題】 もともと暗号化されていないデジタル音楽データや、暗号復号化が行われた後のデジタル音楽データが自由に取扱いえることになると、違法に複製を行ったり頒布することが容易に行えるようになり、音楽文化の発展、ひいてはデジタル音楽産業の発展も妨げることになる。ところが、予め圧縮暗号化されたデジタル音楽データを再生し得るようにしたデジタル音楽再生装置では、圧縮データの伸長にプログラマブルな演算素子を用いるものでも、圧縮データの伸長と暗号の復号化は別個の演算素子を用いて行われていた。すなわち、電気回路に表れているデータバス上に、暗号復号化が行われた後のデータがそのまま流れているのである。別個の演算素子間を結ぶデータバス上を流れるデータを読み取ることは不可能ではなく、暗号復号化が行われた後のデータ、ひいては元のデジタル音楽データが不正に複製されてしまう恐れがある。本発明は、このような従来の技術における課題を鑑みてなされたものであり、暗号復号化が行われた後のデータが回路上から読み取られるのを防止することができるデジタル音楽再生装置を提供するを目的とするものである。

る。

【0004】

【課題を解決するための手段】上述の目的を達成するために、本発明は、圧縮暗号化されたデジタル音楽データについて暗号復号化を行う暗号復号化回路と、前記暗号復号化回路により暗号復号化されたデータを伸長して元のデジタル音楽データを復元する圧縮復元回路とを備え、前記圧縮復元回路により復元されたデジタル音楽データを再生するデジタル音楽データを再生するデジタル音楽再生装置において、前記暗号復号化回路と前記圧縮復元回路とを同一の演算素子内に備え、前記暗号復号化回路により暗号復号化されたデータを前記演算素子の内部バスを通じて前記圧縮復元回路に供給してなることを特徴とするデジタル音楽再生装置として構成されている。本発明に係るデジタル音楽再生装置では、圧縮暗号化されたデジタル音楽データについて暗号復号化を行う暗号復号化回路と、前記暗号復号化回路により暗号復号化されたデータを伸長して元のデジタル音楽データを復元する圧縮復元回路とが同一の演算素子内に備えられ、前記暗号復号化回路により暗号復号化されたデータは、前記演算素子の内部バスを通じて前記圧縮復元回路に供給される。このため、前記暗号復号化回路により暗号復号化されたデータは前記演算素子の外部のバスから直接取得することはできず、暗号復号化が行われた後のデータが回路上から読み取られるのを防止することができる。ただし、たとえ暗号復号化されたデータが前記演算素子の外部のバスから取得できなくとも、前記暗号復号化を行うのに用いる暗号復号化データが、前記演算素子の外部のバスから取得することができれば、圧縮暗号化されたデジタル音楽データから、前記暗号復号化データを用いて元のデジタル音楽データが復元されてしまう恐れが残っている。そこで、前記デジタル音楽再生装置において、例えば前記暗号復号化回路が前記圧縮暗号化されたデジタル音楽データについて暗号復号化を行うのに用いる暗号復号化データを記録する暗号復号化データ記録メモリも前記演算素子内に備え、前記演算素子の内部バスを通じて前記暗号復号化データを前記暗号復号化データ記録メモリから前記暗号復号化回路に供給するようにしてもよい。この場合、暗号復号化を行うのに用いる暗号復号化データも、前記演算素子の外部のバスから取得することはできず、元のデジタル音楽データの複製をより堅固に防止することができる。

【0005】また、前記圧縮復元回路により復元された前記デジタル音楽データは、容量が大きくなって複製に時間がかかるものの、複製されてしまえば、ほとんどオリジナルのものと同一ものが得られることに変わりはない。そこで、前記デジタル音楽再生装置において、例えば前記圧縮復元回路により復元された前記デジタル音楽データをアナログ信号に変換するデジタルアナ

ログ変換器も前記演算素子内に備え、前記圧縮復元回路により復元された前記デジタル音楽データを前記演算素子の内部バスを通じて前記デジタルアナログ変換器に供給するようにしてもよい。この場合、前記圧縮復元回路により復元された前記デジタル音楽データも、前記演算素子の外部のバスからは取得できず、その不正な複製をより困難なものにすることができる。また、前記デジタル音楽再生装置では、複数の圧縮符号化方式に対応するために、前記圧縮復元回路の利用する圧縮復元プログラムが複数用意されることがあるが、揮発性の比較的高速なメモリは高価であるため、コストを抑えようとする、不揮発性の比較的低速なメモリを利用することになる。しかしながら、不揮発性の比較的低速なメモリから前記圧縮復元プログラムを前記圧縮復元回路に供給すると、処理速度が低下してしまう。そこで、前記デジタル音楽再生装置において、例えば前記圧縮復元回路が利用する圧縮復元プログラムを記録する不揮発性の圧縮復元プログラム記録メモリに記録された一部の圧縮復元プログラムを記録する揮発性の圧縮復元プログラム一時記録メモリを前記演算素子内に備え、前記一部の圧縮復元プログラムは前記圧縮復元プログラム一時記録メモリから前記圧縮復元回路に供給するようにしてもよい。この場合、前記圧縮復元プログラム一時記録メモリには、前記圧縮復元プログラム記録メモリに記憶された一部の圧縮復元プログラムを記録するだけの容量を確保すればよく、また前記一部の圧縮復元プログラムは、比較的高速な揮発性の圧縮復元プログラム一時記録メモリから供給されるため、コストを抑えながら高速な処理を実現することができる。

【0006】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態につき説明し、本発明の理解に供する。なお、以下の実施の形態は、本発明の具体的な例であって、本発明の技術的範囲を限定する性格のものではない。ここに、図1は本発明の実施の形態に係るデジタル音楽再生装置の概略構成を示す図である。図1に示す如く、本発明の実施の形態に係るデジタル音楽再生装置は、デジタル音楽データ記録メモリ101、演算素子102、圧縮復元プログラム記録メモリ103、D/A変換器104、及びアナログ回路105などからなる。デジタル音楽データ記録メモリ101は、圧縮暗号化されたデジタル音楽データを格納するためのメモリであり、演算素子102に接続されている。演算素子102は、デジタル音楽データ記録メモリ101からのデジタル音楽データを、圧縮暗号化される前の元のデジタル音楽データに復元する処理を行うものであり、D/A変換器104に接続されている。圧縮復元プログラム記録メモリ103は、演算素子102の外部に接続されており、前記デジタル音楽データを圧縮符号化された圧縮復元プログラムに対応する復元データに圧縮復元

プログラムを演算素子102に供給する。D/A変換器104は、演算素子102から供給されたデジタル音楽データをアナログ信号に変換するものであり、アナログ回路105に接続されている。アナログ回路105は、D/A変換器104とスピーカとを接続し、必要に応じて増幅などの処理を行ってから、D/A変換104からのアナログ信号をスピーカに入力する。

【0007】本発明の実施の形態に係るデジタル音楽再生装置の主要部となるのが、上述した各構成のうちの演算素子102である。演算素子102の内部構成も図1に示している。図1に示す如く、演算素子102は、その内部にデータ入力回路11、暗号復号化回路12、圧縮復元回路13、データ出力回路、暗号復号化データ記録メモリ21を含む。データ入力回路11は、デジタル音楽データ記録メモリ101と接続され、デジタル音楽データ記録メモリ101から圧縮暗号化されたデジタル音楽データを演算素子102に入力するためのインターフェースである。暗号復号化回路12は、データ入力回路11から入力された圧縮暗号化されたデジタル音楽データの暗号を、暗号復号化データ記録メモリ21に記録された暗号復号化データを用いて復号化する回路である。圧縮復元回路13は、圧縮復元プログラム記録メモリ103に記録された圧縮復元プログラムを用いて、暗号復号化回路12によって暗号復号化されたデータを伸長して圧縮前の元のデジタル音楽データを復元する回路である。データ出力回路11は、圧縮復元回路13により得られたデジタル音楽データをD/A変換器104に出力するためのインターフェースである。また、暗号復号化データ記録メモリ21は、暗号復号化のための暗号復号化データを記録するメモリであり、前記暗号復号化データを暗号復号化回路12に供給する。例えばDESによる共通鍵暗号化方式を用いる場合には、暗号復号化データ記録メモリ21には、DES暗号のためのパラメータデータ及び、暗号処理側と共通の秘密とすべき共通鍵が記録される。上述のような演算素子102内の各構成は内部バス（図1では便宜上前記演算素子102内にある矢印で表している）によって接続されており、演算素子102外部の接続路から得られるのは、データ入力回路11に入力されるデータとデータ出力回路14から出力されるデータ、圧縮復元プログラムのみである。暗号復号化回路12から出力されるデータは、圧縮されてはいるものの暗号化されておらず、よく利用される圧縮符号化方式は限られているから、元のデジタル音楽データを復元するのは簡単であり、また比較的データの容量も小さいため複製も容易である。このようなデータも、演算素子102の内部バスのみを通過し、外部から隠蔽される。また、暗号復号化データ記録メモリ21に記録されている暗号復号化データも、内部バスのみを通過し、外部から隠蔽される。暗号復号化データ記録メモリ21の暗号復号化データバスに取得さ

れれば、圧縮暗号化されたデジタル音楽データしか得られなくとも、それから簡単に元のデジタル音楽データが復元されてしまうことになるが、暗号復号化データも外部から隠蔽することによって、そのような事態も防止される。このように、本発明の実施の形態に係るデジタル音楽再生装置では、暗号復号化回路と圧縮復元回路とが同一の演算素子内に設けられており、前記暗号復号化回路により暗号復号化されたデータが前記演算素子の内部バスを通じて前記圧縮復元回路に供給されるため、暗号復号化が行われたデータが回路上から読み取られるのを防止することができる。さらに、前記暗号復号化データ記憶メモリも前記演算素子内に備えられ、前記演算素子の内部バスを通じて前記暗号復号化データが前記暗号復号化データ記憶メモリから前記暗号復号化回路に供給されるため、圧縮暗号化されたデータから元のデジタル音楽データを復元するのに必要となる前記暗号復号化データも外部から隠蔽することができる。

【0008】

【実施例】前記実施の形態では、演算素子102の外部に配置された圧縮復元プログラム記録メモリ103から直接圧縮復元回路13に前記圧縮復元プログラムが供給されていたが、例えば図2に示す如く、前記圧縮復元プログラムを一時的に記録する揮発性の圧縮復元プログラム一時記録メモリ31を演算素子102内に設け、圧縮復元プログラム記録メモリ103に複数記憶されている前記圧縮復元プログラムのうちの必要な前記圧縮復元プログラムは圧縮復元プログラム一時記録メモリ31に記憶させておき、当該圧縮復元プログラムは圧縮復元プログラム一時記録メモリ31を通じて圧縮復元回路13に供給するようにしてもよい。より高速な処理を行うために、高速なメモリから前記圧縮復元プログラムを読み出すことが好ましいが、揮発性の高速なメモリは高価であり、多くの前記圧縮復元プログラムを記憶するために必要な容量を確保しようとすると、コストを抑えることが困難になる。一方、不揮発性の低速なメモリは比較的安価であるから、圧縮復元プログラム記録メモリ103の容量を増大させてもコストを抑えることができる。そこで、圧縮復元プログラム記録メモリ103に記憶されているいずれか、又は一部の前記圧縮復元プログラムだけを記憶する容量を圧縮復元プログラム一時記録メモリ31に確保しておき、圧縮復元回路13が利用する前記圧縮復元プログラムは圧縮復元プログラム一時記録メモリ31から供給する。圧縮復元プログラム記録メモリ103の容量が少数の圧縮復元プログラムを格納できる程度であれば、コストの増大もそれほど小さくなく、コストを抑えながら高速な処理を実現することができる。また、前記実施の形態では、演算素子102の外部にD/A変換器104が配置されていたが、例えば図3に示す如く、D/A変換器104も演算素子102内部に設け、データ出力回路14から出力されるデジタル音楽

データを演算素子102の内部バスを通じてD/A変換器41に供給するようにしてもよい。データ出力回路14から出力される前記デジタル音楽データは、容量が大きくなって複製に時間がかかるものの、複製されてしまえば、ほとんどオリジナルのものと同じものが得られることに変わりはない。従って、データ出力回路14から出力されるデジタル音楽データを演算素子102の内部バスを通じてD/A変換器41に供給することによって、前記デジタル音楽データも隠蔽する。これによって、不正な複製をより困難なものにすることができる。

【0009】

【発明の効果】以上説明した通り、本発明に係るデジタル音楽再生装置によれば、圧縮暗号化されたデジタル音楽データについて暗号復号化を行う暗号復号化回路と、前記暗号復号化回路により暗号復号化されたデータを伸長して元のデジタル音楽データを復元する圧縮復元回路とが同一の演算素子内に備えられ、前記暗号復号化回路により暗号復号化されたデータは、前記演算素子の内部バスを通じて前記圧縮復元回路に供給されるため、暗号復号化された後のデータが回路上から読み取られるのを防止することができる。また、前記デジタル音楽再生装置において、例えば前記暗号復号化回路が前記圧縮暗号化されたデジタル音楽データについて暗号復号化を行うのに用いる暗号復号化データを記録する暗号復号化データ記録メモリも前記演算素子内に備え、前記演算素子の内部バスを通じて前記暗号復号化データを前記暗号復号化データ記録メモリから前記暗号復号化回路に供給すれば、暗号復号化を行うのに用いる暗号復号化データも、前記演算素子の外部のバスから取得することはできず、元のデジタル音楽データの複製をより堅固に防止することができる。さらに、前記デジタル音

楽再生装置において、例えば前記圧縮復元回路により復元された前記デジタル音楽データをアナログ信号に変換するデジタルアナログ変換器も前記演算素子内に備え、前記圧縮復元回路により復元された前記デジタル音楽データを前記演算素子の内部バスを通じて前記デジタルアナログ変換器に供給すれば、前記圧縮復元回路により復元された前記デジタル音楽データも、前記演算素子の外部のバスからは取得できず、その不正な複製をより困難なものにすることができる。さらに、前記デジタル音楽再生装置において、例えば前記圧縮復元回路が利用する圧縮復元プログラムを記録する不揮発性の圧縮復元プログラム記録メモリに記録された一部の圧縮復元プログラムを記録する揮発性の圧縮復元プログラム一時記録メモリを前記演算素子内に備え、前記一部の圧縮復元プログラムは前記圧縮復元プログラム一時記録メモリから前記圧縮復元回路に供給すれば、コストを抑えながら高速な処理を実現することができる。

【図面の簡単な説明】

【図1】 本発明の実施の形態に係るデジタル音楽再生装置の概略構成を示す図。

【図2】 本発明の一実施例に係るデジタル音楽再生装置の概略構成を示す図。

【図3】 本発明の他の実施例に係るデジタル音楽再生装置の概略構成を示す図。

【符号の説明】

12…暗号復号化回路

13…圧縮復元回路

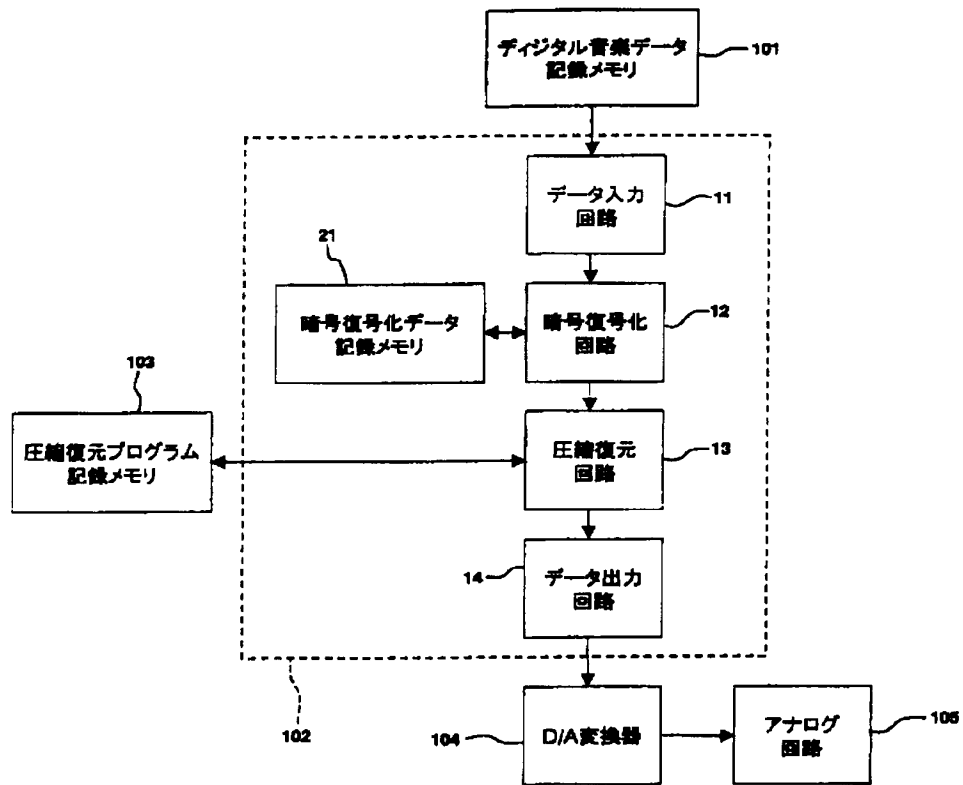
21…暗号復号化データ記録メモリ

31…圧縮復元プログラム一時記録メモリ

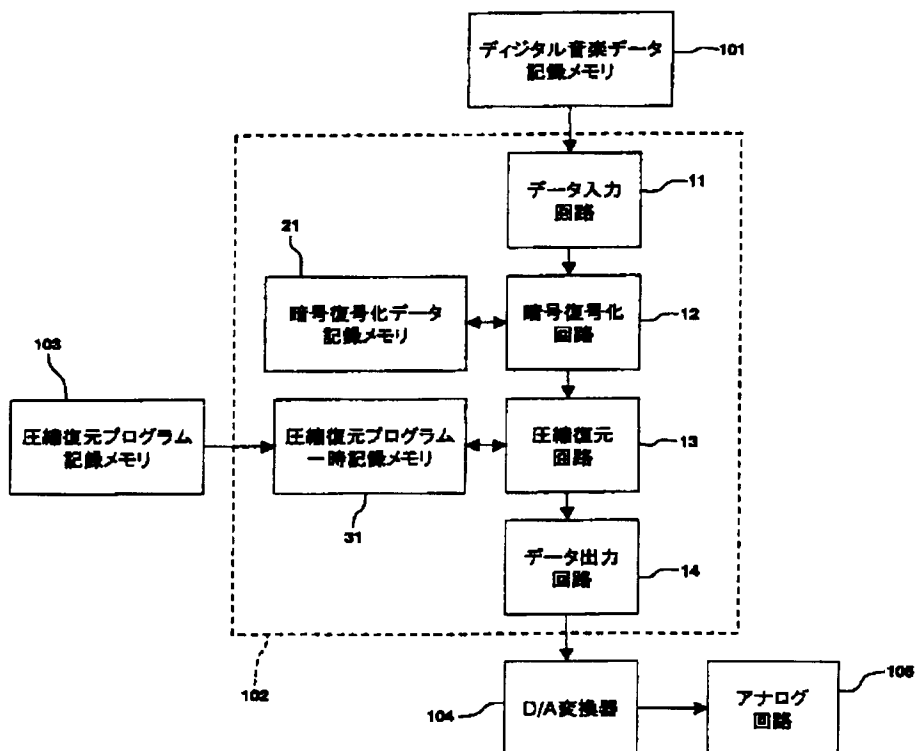
102…演算素子

104…D/A変換器

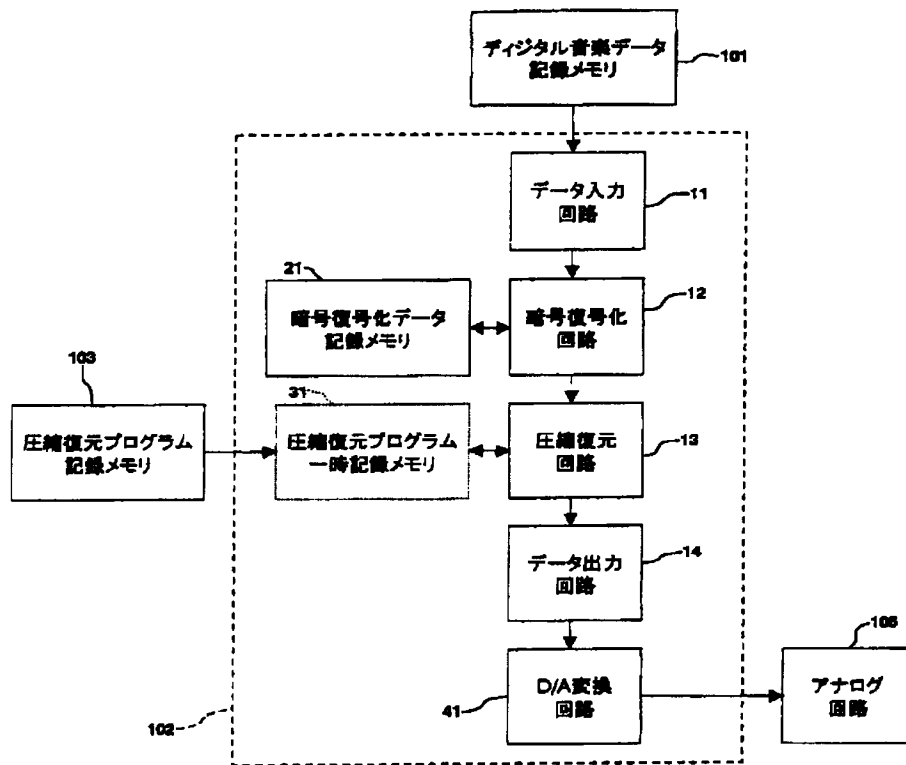
【図 1】



【図 2】



【図 3】



【手続補正書】

【提出日】平成13年8月3日（2001. 8. 3）

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 圧縮暗号化されたデジタル音楽データについて暗号復号化を行う暗号復号化回路と、前記暗号復号化回路により暗号復号化されたデータを伸長して元のデジタル音楽データを復元する圧縮復元回路とを備え、前記圧縮復元回路により復元されたデジタル音楽データを再生するデジタル音楽再生装置において、前記暗号復号化回路と、前記圧縮復元回路と、該圧縮復元回路が利用する圧縮復元プログラムを記録する不揮発性の圧縮復元プログラム記録メモリに記録された一部の圧縮復元プログラムを記録する揮発性の圧縮復元プログラム一時記録メモリと、を同一の演算素子内に備え、前記暗号復号化回路により暗号復号化されたデータは前記演算素子の内部バスを通じて前記圧縮復元回路に供給し、前記一部の圧縮復元プログラムは前記圧縮復元プログラムの一時記録メモリから前記圧縮復元回路に供給される

ことを特徴とするデジタル音楽再生装置。

【請求項2】 前記暗号復号化回路が前記圧縮暗号化されたデジタル音楽データについて暗号復号化を行うのに用いる暗号復号化データを記録する暗号復号化データ記録メモリも前記演算素子内に備え、前記演算素子の内部バスを通じて前記暗号復号化データを前記暗号復号化データ記録メモリから前記暗号復号化回路に供給してなる請求項1記載のデジタル音楽再生装置。

【請求項3】 前記圧縮復元回路により復元された前記デジタル音楽データをアナログ信号に変換するデジタルアナログ変換器も前記演算素子内に備え、前記圧縮復元回路により復元された前記デジタル音楽データを前記演算素子の内部バスを通じて前記デジタルアナログ変換器に供給してなる請求項1又は2記載のデジタル音楽再生装置。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0004

【補正方法】変更

【補正内容】

【0004】

【課題を解決するための手段】 上述の目的を達成するため

めに、本発明は、圧縮暗号化されたデジタル音楽データについて暗号復号化を行う暗号復号化回路と、前記暗号復号化回路により暗号復号化されたデータを伸長して元のデジタル音楽データを復元する圧縮復元回路とを備え、前記圧縮復元回路により復元されたデジタル音楽データを再生するデジタル音楽データを再生するデジタル音楽再生装置において、前記暗号復号化回路と、前記圧縮復元回路と、該圧縮復元回路が利用する圧縮復元プログラムを記録する不揮発性の圧縮復元プログラム記録メモリに記録された一部の圧縮復元プログラムを記録する揮発性の圧縮復元プログラム一時記録メモリとを同一の演算素子内に備え、前記暗号復号化回路により暗号復号化されたデータを前記演算素子の内部バスを通じて前記圧縮復元回路に供給し、前記一部の圧縮復元プログラムは前記圧縮復元プログラム一時記録メモリから前記圧縮復元回路に供給してなることを特徴とするデジタル音楽再生装置として構成されている。本発明に係るデジタル音楽再生装置では、圧縮暗号化されたデジタル音楽データについて暗号復号化を行う暗号復号化回路と、前記暗号復号化回路により暗号復号化されたデータを伸長して元のデジタル音楽データを復元する圧縮復元回路とが同一の演算素子内に備えられ、前記暗号復号化回路により暗号復号化されたデータは、前記演算素子の内部バスを通じて前記圧縮復元回路に供給される。このため、前記暗号復号化回路により暗号復号化されたデータは前記演算素子の外部のバスから直接取得することはできず、暗号復号化が行われた後のデータが回路上から読み取られるのを防止することができる。また、前記デジタル音楽再生装置では、複数の圧縮符号化方式に対応するために、前記圧縮復元回路の利用する圧縮復元プログラムが複数用意されることがあるが、揮発性の比較的高速なメモリは高価であるため、コストを抑えようとすると、不揮発性の比較的低速なメモリを利用することになる。しかしながら、不揮発性の比較的低速なメモリから前記圧縮復元プログラムを前記圧縮復元回路に供給すると、処理速度が低下してしまう。しかし上記発明によれば、前記圧縮復元プログラム一時記録メモリには、前記圧縮復元プログラム記録メモリに記憶された一部の圧縮復元プログラムを記録するだけの容量を確保すればよく、また前記一部の圧縮復元プログラム

は、比較的高速な揮発性の圧縮復元プログラム一時記録メモリから供給されるため、コストを抑えながら高速な処理を実現することができる。ただし、たとえ暗号復号化されたデータが前記演算素子の外部のバスから取得できなくとも、前記暗号復号化を行うのに用いる暗号復号化データが、前記演算素子の外部のバスから取得することができれば、圧縮暗号化されたデジタル音楽データから、前記暗号復号化データを用いて元のデジタル音楽データが復元されてしまう恐れが残っている。そこで、前記デジタル音楽再生装置において、例えば前記暗号復号化回路が前記圧縮暗号化されたデジタル音楽データについて暗号復号化を行うのに用いる暗号復号化データを記録する暗号復号化データ記録メモリも前記演算素子内に備え、前記演算素子の内部バスを通じて前記暗号復号化データを前記暗号復号化データ記録メモリから前記暗号復号化回路に供給するようにしてもよい。この場合、暗号復号化を行うのに用いる暗号復号化データも、前記演算素子の外部のバスから取得することはできず、元のデジタル音楽データの複製をより堅固に防止することができる。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0005

【補正方法】変更

【補正内容】

【0005】また、前記圧縮復元回路により復元された前記デジタル音楽データは、容量が大きくなって複製に時間がかかるものの、複製されてしまえば、ほとんどオリジナルのものと同じものが得られることに変わりはない。そこで、前記デジタル音楽再生装置において、例えば前記圧縮復元回路により復元された前記デジタル音楽データをアナログ信号に変換するデジタルアナログ変換器も前記演算素子内に備え、前記圧縮復元回路により復元された前記デジタル音楽データを前記演算素子の内部バスを通じて前記デジタルアナログ変換器に供給するようにしてもよい。この場合、前記圧縮復元回路により復元された前記デジタル音楽データも、前記演算素子の外部のバスからは取得できず、その不正な複製をより困難なものにすることができる。

フロントページの続き

(72)発明者 下田 敏章
兵庫県神戸市西区高塚台 1 丁目 5 番 5 号
株式会社神戸製鋼所神戸総合技術研究所内

Fターム(参考) 5D044 AB05 BC03 FG10 FG18 GK07
HL08 HL09
5D045 DA20
5J064 AA00 BC01 BC02 BC07 BD03